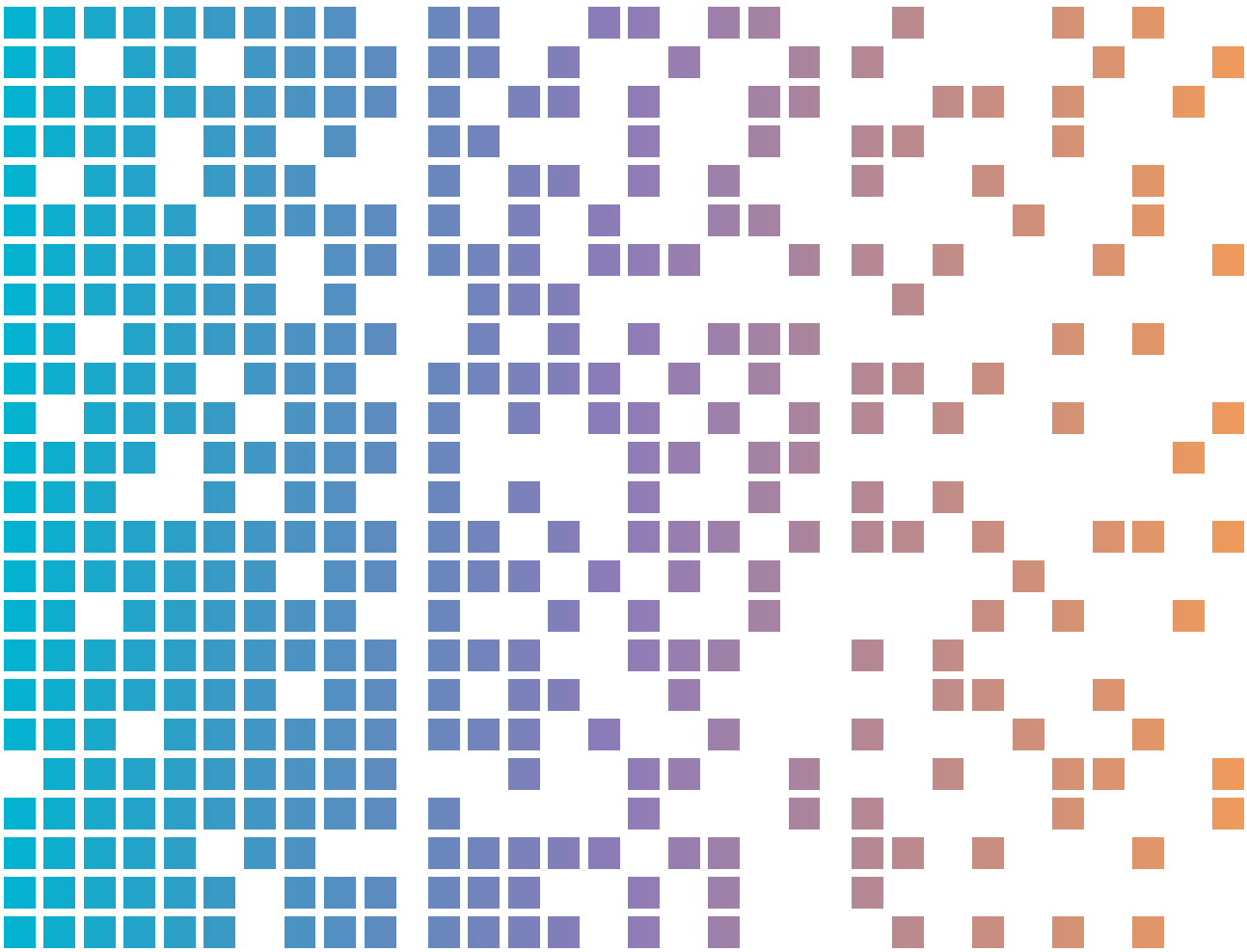
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

静かに進行する情報窃取：サイバー犯罪者が情報窃取型マルウェアを使って企業ネットワークを侵害



内容の難易度
中程度 ●●○

目次

目的

情報窃取型マルウェアは、ユーザーの認証情報やシステム情報を取得し、サイバー犯罪者によって主に金銭的利益を目的として悪用されます。情報窃取型マルウェアは、オーストラリアを含む世界中のさまざまな組織や業種を標的としたサイバー犯罪攻撃で確認されています。本資料では、情報窃取型マルウェアに関するサイバーセキュリティのガイダンスを提供しており、脅威活動の状況や、組織および従業員向けの緩和策についても紹介しています。

要点

- 情報窃取型マルウェア（インフォスティーラーとも呼ばれます）は、被害者のデバイスから情報を収集するように設計されたマルウェアの一種です。これには、ユーザー名やパスワード、クレジットカード情報、暗号通貨ウォレット、ローカルファイルに加え、クッキーや閲覧履歴、自動入力フォームの情報などのブラウザデータが含まれます。
- サイバー犯罪者は、企業アカウントに関連付けられた盗まれたユーザー認証情報を購入・悪用し、被害者の雇用先やその顧客、その他の企業システムへの初期アクセスを狙うことがあります。これらの組織が受ける影響としては、ランサムウェア攻撃や恐喝、ビジネスメール詐欺（BEC）、知的財産の窃取などが挙げられます。
- オーストラリア信号局（ASD）傘下のオーストラリア・サイバーセキュリティセンター（ACSC）（以下、「ASD-ACSC」）は、従業員が侵害された個人デバイスから業務用リソースにアクセスしたことで発生した、企業ネットワーク侵害の事例を確認しています。複数の事例で、サイバー犯罪者は盗まれた有効なユーザー認証情報を悪用し、企業ネットワークへの初期アクセスを取得しています。調査の結果、サイバー犯罪者が特権ユーザーアカウントへのアクセスに成功した後に、大規模な侵害が発生するケースが多いことが明らかになりました。
- 従業員、契約業者、マネージドサービスプロバイダー、その他の関係者に対し、BYOD（私物端末）を含むハードウェアでネットワークへのリモートアクセスを提供している組織は、情報窃取型マルウェアのリスクを認識し、この脅威から自らを保護する必要があります。サイバー犯罪者は、フィッシングメール、海賊版ソフトウェアのダウンロード、検索エンジン最適化（SEO）手法、悪意のある広告、ソーシャルメディア上に投稿された不正なリンクなど、さまざまな手法を用いて情報窃取型マルウェアを被害者のデバイスに展開します。一般的に、業務と個人利用の両方に使用されるデバイスは、ユーザーの行動やセキュリティ対策の不足により、これらの手法による感染リスクが高くなります。
- インフォスティーラーは、特にサイバー犯罪の初心者や技術力の限られた犯罪者にとって、サイバー犯罪を収益化する魅力的な手段となっています。一部のサイバー犯罪者は、インフォスティーラー製品を「マルウェア・アズ・ア・サービス（MaaS）」の形式で提供し、使用料として月額のサブスクリプション料金を課しています。

背景

サイバー犯罪者によるインフォスティーラーの使用は、オーストラリアの組織のセキュリティや健全な運営に対する脅威となっています。インフォスティーラーの感染は、サイバー犯罪者がユーザー認証情報を収集する手段として用いることから、大規模なサイバーセキュリティインシデントの前兆としてよく見られます。これらのユーザー認証情報、特にインターネット経由でアクセス可能なリモートサービスや特権アカウントへのアクセス権を持つ情報は、その後、企業のシステムやデータへの初期アクセスを可能にするために悪用されます。

備考：初期アクセスブローカーは、サイバー犯罪のエコシステムにおいて、盗まれたユーザー認証情報を購入し、その有効性を確認するという特化した役割を担っています。その後、狙われやすい企業環境を標的とするサイバー犯罪者に、高品質なユーザー認証情報をオークション形式で販売します。サイバー犯罪者は、これらの認証情報を利用して組織のネットワークに侵入し、不正行為を行います。

盗まれた有効なユーザー認証情報は、企業ネットワークやエンタープライズシステムへの迅速な初期アクセスを可能にするため、サイバー犯罪者にとって非常に価値があります。盗まれた有効なユーザー認証情報を用いることで、サイバー犯罪者は以下のような一般的な戦術や手法を使わずに済むようになります。

- 標的の特定および調査
- 標的のネットワークに存在する脆弱性の列挙
- 以下のような初期アクセスのための手段を開発する：
  - フィッシング用の素材
  - ソフトウェアの脆弱性の悪用
  - リモートデスクトッププロトコル（RDP）や仮想プライベートネットワーク（VPN）サービスなどのリモートサービスの標的化
  - ユーザー認証情報に対するブルートフォース攻撃（パスワードの推測）

これらの手順には時間の投資や一定の技術的スキルが求められるため、一部のサイバー犯罪者にとっては障壁となります。特に、企業ネットワークの防御を突破できないサイバー犯罪者にとっては、インフォスティーラーによる感染は非常に役立ちます。なぜなら、このマルウェアによって、標的とする企業ネットワークへのアクセスに必要なユーザー認証情報を迅速かつ容易に入手できるからです。

リモートワーク環境では、一部の従業員が仕事とプライベートの両方で私用デバイスを使用しています。その際、従業員はウェブブラウザのパスワード保存機能や拡張機能にユーザー認証情報を保存したり、ブラウザの自動入力機能を利用したりする場合があります。インフォスティーラーは、ブラウザに保存されたパスワードに加え、認証クッキーやブラウザ内のその他の個人データも標的にします。

企業のデバイスとは異なり、私用デバイスには企業のセキュリティポリシーが必ずしも適用されていないため、組織にとってリスクが高くなります。例えば、従業員が海賊版ソフトウェアのダウンロードやリスクの高いオンライン閲覧などの行為を行うことで、サイバー脅威やマルウェア感染のリスクが高くなります。

インフォスティーラー、配布者、初期アクセスブローカー、そしてランサムウェアのアフィリエイトは、現在、金銭的利益を目的としたサイバー犯罪エコシステムの中核を成しています。サイバー犯罪者が攻撃の特定の段階に特化し、その能力を開発したうえで、他の犯罪アフィリエイトにサービスとして提供・販売することで、サイバー犯罪のエコシステムはさらに効率的に拡大していきます。

脅威活動

ASD-ACSCは、インフォスティーラーの活動が世界的に増加している状況を継続的に追跡・監視しています。こうした活動の増加は、オーストラリアのネットワークに対する脅威の高まりを示しています。業界の報告によると、インフォスティーラーは2023年を通じて、サイバー犯罪活動において最も多く使用されたマルウェアの一種でした。ダークウェブのマーケットプレイスにおける盗難データの販売量の増加や、それらのデータを利用する初期アクセスブローカーの活動の活発化は、このような動きの拡大を示しており、2024年に入ってさらに加速しています。

インフォスティーラーのエコシステム

ステージ1：マルウェアの入手

インフォスティーラーは通常、サイバー犯罪者向けのマーケットプレイスで、MaaSやStealer-as-a-Service（スティーラー・アズ・ア・サービス）として提供されるか、ソースコードの形で販売されます。MaaSとは、マルウェア開発者が自身の悪意あるソフトウェアを、正規のSaaS（ソフトウェア・アズ・ア・サービス）と同様に、ウェブベースのプラットフォームを通じてサブスクリプション形式で個人に提供・販売するビジネスモデルのことを指します。MaaSモデルは、広範な技術的スキルを持たない個人でもマルウェアを配布し、サイバー攻撃に利用するための盗難情報を収集できるようにすることで、サイバー犯罪のハードルを下げています。

MaaSとして提供されるインフォスティーラーは、比較的安価な月額料金で提供されるのが一般的であり、サイバー犯罪者にはインフォスティーラー専用のダッシュボードが用意されます。このダッシュボードは、インフォスティーラーマルウェアの作成を容易にし、盗んだデータの整理や、侵害したシステムの数の追跡を可能にします。MaaSの運営者は、ウイルス対策ソフトウェアによる検出を回避し、加入者を引き付け、維持するために、機能アップデート、ツール、技術サポートを提供しています。多くのインフォスティーラーは、データを窃取した後、被害者のデバイスから自らを削除する機能を備えています。

ステージ2：配布

インフォスティーラーを配布し、侵害したデバイスから情報を収集するサイバー犯罪者は、「トラッファー（トラフィック配布者）」と呼ばれています。トラッファーは被害者を悪意のあるリンクへ誘導し、広範なキャンペーンの一環としてインフォスティーラーの拡散を促進します。ほとんどのキャンペーンは無差別に実行されており、機会に乗じた感染に依存しています。しかし、キャンペーンの中には、特定の業界に特化し、特定の被害者をターゲットにしたスピアフィッシングを行うものもあります。トラッファーは、例えば、特定の高価値な組織や業界へのアクセスを求める顧客の要望に応じて、こうしたより標的を絞ったキャンペーンを実行します。

トラッファーは、以下のような多様な手法を用いて、被害者のデバイスにインフォスティーラーを感染させます。

- **ボットネット**：サイバー犯罪者が制御する侵害されたコンピュータシステムのネットワークにおいて、フィッシングメッセージやマルウェアの配布などの悪意ある行為をするために利用されます。

- **フィッシング**：メールやソーシャルメディア、フォーラム、メッセージアプリなどを通じて、詐欺的手法により機密情報を取得しようとする行為。これらは一般的な配布手段であり、サイバー犯罪者にとっての参入障壁を下げる要因となっています。
  - これらのメッセージには、悪意のあるファイルが直接添付されるのではなく、悪意のあるリンクが含まれていることが一般的です。
- **悪意のある検索結果**：検索エンジン最適化（SEO）技術を利用して、標的を正規のソフトウェアや他のコンテンツに見せかけたマルウェアを配布するウェブサイトへ誘導する手法。
- **マルバタイジング**：正規のオンライン広告に悪意のあるコードを埋め込み、マルウェアを配布する手法。
- **クラック版や海賊版ソフトウェア**：YouTubeの動画説明欄やコメントに記載された悪意のあるリンク、あるいは信頼性の低いダウンロードサイトを通じて共有される、ビデオゲームなどのダウンロードコンテンツ。
- **ソーシャルメディアの広告や投稿**：ユーザーを偽装されたマルウェアファイルへと誘導する手法。
- **悪意のあるソフトウェアアップデート**：多くの場合、ウェブブラウザのアップデートに偽装されています。

ステージ3：データ収集

インフォスティーラーは、被害者のデバイスで実行されると、その端末から機密データの収集を始めます。インフォスティーラーがボットネットの一部として機能している場合、サイバー犯罪者はユーザー認証情報の窃取にとどまらず、設定コマンドを送信して追加機能を有効化したり、別のマルウェアを送り込んだりすることで、侵害したデバイスを遠隔操作することができます。一般的に、インフォスティーラーは以下の情報を窃取することができます。

- ユーザー名やパスワード、特にウェブブラウザに保存された多要素認証（MFA）のユーザーセッションやトークン
- 認証クッキー
- ウェブブラウザの自動入力フォームに保存された情報
- 電子メールの認証情報、内容、連絡先情報
- ウェブ閲覧履歴
- ユーザーのドキュメント
- クレジットカード情報
- デスクトップのメッセージングアプリのチャットログ
- システム情報
- 暗号通貨ウォレット
- VPNやファイル転送プロトコル（FTP）の認証情報 。

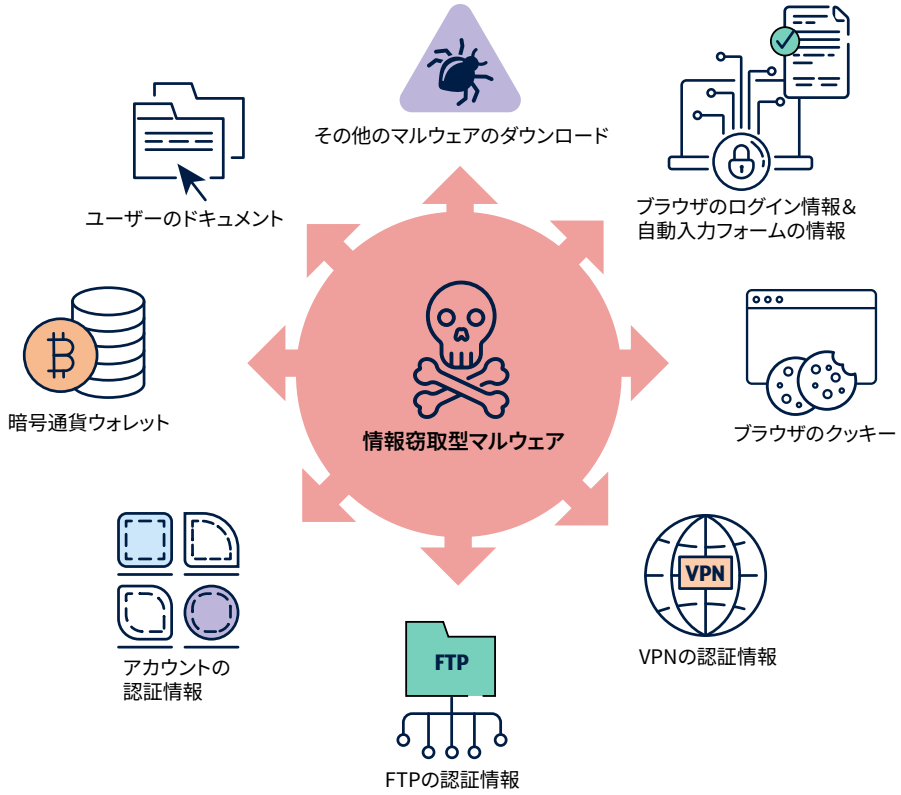


図1. インフォスティーラーの機能

一部のウェブブラウザの認証クッキーは、ユーザーが再認証しなくても済むように、数日間にわたってアカウントやサービスへのログイン状態を維持します。これらの認証クッキーが盗まれると、MFAの要件を事実上回避できるため、サイバー犯罪者は被害者のアカウントや企業ネットワーク、エンタープライズシステムに不正アクセスできるようになります。

ステージ4：データの集約と収益化

インフォスティーラーは、被害者の情報（「ログ」と呼ばれる）を悪意のあるコマンド&コントロールサーバーに流出させるように設定されています。一般的に、インフォスティーラーはTelegramやDiscordなどの人気メッセージングアプリを利用して、収集したログのフィードをサイバー犯罪者と共有します。

Telegramやダークウェブ上には、ログの売買や取引を専門とするマーケットプレイスが存在します。サイバー犯罪者は、ログを以下のようなさまざまな方法で収益化します。

- ログを犯罪マーケットプレイスで販売する（初期アクセスブローカーへの販売を含む）
- 個人情報の窃盗や恐喝により、被害者から直接搾取する
- ランサムウェア活動のために、企業ネットワークへの初期アクセスに情報を活用する 。

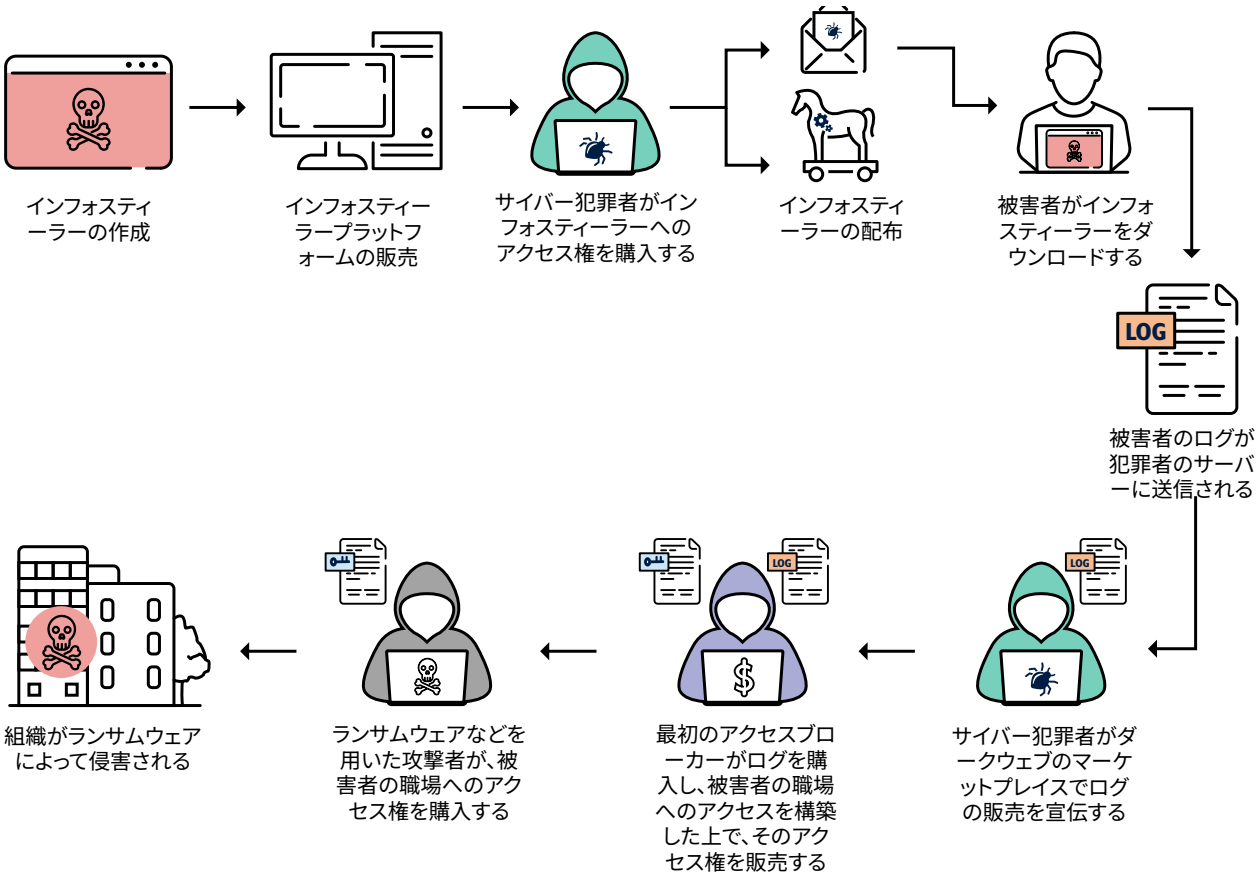


図2. インフォスティーラーのエコシステムとそれが組織に及ぼす影響

影響

インフォスティーラーは、個人と組織の双方に深刻な影響を及ぼす可能性があります。インフォスティーラーによってユーザー認証情報が収集されると、サイバー犯罪者はそれらの有効なアカウントを用いて企業ネットワークやエンタープライズシステムにアクセスする可能性があります。この場合、システム管理者による検知が遅れることがよくあります。

インフォスティーラーの被害を受けた**組織**には、以下のような影響が生じる可能性があります。

- ランサムウェア
- データ漏えい
- ビジネスメール詐欺
- 知的財産の窃取
- 機密情報の窃取 。

インフォスティーラーの被害を受けた**個人**には、以下のような影響が及ぶ可能性があります。

- 個人のメールアカウントやソーシャルメディアアカウントへの不正アクセス
- 個人情報盗用のリスクの増大
- フィッシング攻撃のリスクの増大
- 金銭的損失や金融口座の不正アクセス
- プライバシーの侵害 。

ケーススタディ

このケーススタディは、一般公開を可能にするために匿名化されています。本事例は、ASD-ACSCに報告された、オーストラリアの組織に影響を及ぼした複数のサイバーセキュリティインシデントを基に作成されています。影響を受けた組織は、以下「当該組織」と記載します。本事例に登場する個人名はすべて架空のものであり、被害者の身元を保護するために詳細情報は削除されています。

当該組織は、従業員が私用デバイスから社内システムへアクセスすることを認めているオーストラリア企業です。「アリス」は当該組織に所属し、リモートワークをしている従業員です。

アリスは在宅勤務中、私用のノートパソコンを使って当該組織の社内ネットワークにリモートアクセスします。アリスは、**自身のノートパソコン**に、正規のサイトだと信じていたウェブサイトからNotepad++（メモ作成ソフトの一種）を**ダウンロード**しました。**インフォスティーラー**が、Notepad++ソフトウェアのインストーラーに偽装されていました。

アリスがソフトウェアをインストールしようとした際、インフォスティーラーが起動し、彼女のノートパソコンから**ユーザー認証情報の収集**を開始しました。これには、彼女がウェブブラウザの保存ログイン機能に保存していた仕事用のユーザー名とパスワードも含まれていました。その後、インフォスティーラーはこれらのユーザー認証情報を、サイバー犯罪グループが管理する遠隔のコマンド＆コントロールサーバーに送信しました。

盗まれたログは他のログとまとめられ、ダークウェブのマーケットプレイスを通じて**サイバー犯罪者に販売**されました。

サイバー犯罪者の「ボブ」は、アリスのユーザー認証情報を購入し、その中から当該組織のネットワーク上のサービスにアクセス可能な認証情報を特定しました。アリスの所属する組織ではこれらのサービスに**MFAが設定されていなかった**ため、ボブは盗んだユーザー認証情報だけで**認証に成功し、企業ネットワークにアクセス**することができました。

ボブは、盗んだ**有効なユーザー認証情報**を使って、アリスの所属する組織の企業ネットワークに検知されることなくアクセスしました。ボブは企業ネットワーク内を横断的に移動し、当該組織の機密データを特定したうえで、それを抽出し、企業を脅迫するために利用しました。

機密データを盗んだ後、ボブは当該組織の**データベースやファイルシステム**を**暗号化**し、アクセス不能な状態にしました。

緩和策

組織は、自社の企業ネットワークに接続するデバイス、特にリモートワーク中の従業員が使用する私用デバイスに対しては、管理を強制できない場合があります。ASD-ACSCは、インフォスティーラーによるユーザー認証情報の窃取リスクから組織を保護するために、各組織が対策の実施に重点を置くことを推奨しています。これらの緩和策には以下が含まれます。

従業員にサイバーセキュリティに関する意識向上の研修を実施する

- 効果的な研修を従業員に実施することで、標的型のソーシャルエンジニアリングや悪意のあるファイルのダウンロードを未然に防ぐ。
- インフォスティーラー、その配布手法、および組織に対するフィッシングの脅威についての認識を高める。

企業アカウントを保護する

- MFAを導入する
- 外部・内部のサービスやシステム、機密データのリポジトリ全般にわたり、MFAを導入する（ウェブメール、VPN、重要なシステムにアクセスする特権ユーザーアカウントについては特に）。すべてのアカウントにフィッシング耐性のあるMFAを導入することが、ベストプラクティスとされています。
- 不要になったユーザーアカウントは無効化する。
- 管理者権限を制限する
- ネットワーク管理やその他の特権作業は、専用の制限されたワークステーション（いわゆるセキュアな管理用ワークステーション）でのみ実施する。
- 最小権限の原則に従い、システム管理には特権ユーザーアカウントを、通常業務には一般ユーザーアカウントを使用させる。
- 特権ユーザーアカウントについては、明示的に許可されたものを除き、インターネット、電子メール、ウェブサービスへのアクセスを禁止する。
- システムやアプリケーションに対して、「ジャストインタイム管理（必要な時にのみ特権を付与する）」の導入を検討する。
- 特権ユーザーアカウントの管理と監査を徹底する。
- パスワードは定期的に更新する。特に外部に公開されているリモートアクセス用アカウントについてはこれを徹底する。
- セッショントークンやクッキーには、有効期限の設定やサンセットポリシー（一定期間後の無効化）を適用する。

エンタープライズモビリティを強化する

- エンタープライズモビリティに関するリスクアセスメントを実施し、エンタープライズモビリティ強化のためのガイドラインを適用する。
- 従業員が業務に私用デバイスを使用することを認める場合は、BYOD（私用デバイスの業務利用）ポリシーを導入する。企業が管理するデバイスは、管理されていない私用デバイスよりもセキュリティが高いためである。

ネットワークにアクセスするベンダー、特にSaaS（ソフトウェア・アズ・ア・サービス）ベンダーやマネージドサービスプロバイダーによるサプライチェーンリスクを確認・評価する。マネージドサービスプロバイダーを利用する際のセキュリティ管理方法。

企業ネットワークを保護する

- アプリケーションやオペレーティングシステムを常に最新の状態に保つ。
- ローカルセキュリティポリシーを適用し、厳格な許可リストによるアプリケーション管理を実施する。
- ネットワークセグメンテーションを実施し、役割や機能に応じてネットワークを分割する。
- ユーザーの活動を監査・監視する。特にリモート勤務の従業員についてはこれを徹底する。
- 特権アカウントを監視することで、機密データへの不正アクセスや、外部ネットワークへの大量データのアップロードなどの異常なデータ転送活動を検知することができる。
- 不正なデータ転送を防止するため、データ損失防止ポリシーやツールを導入する。

ASDのサイバーセキュリティネットワークパートナーになり、ASDのサイバー脅威インテリジェンス共有（CTIS）サービスに加入する。

- CTISは、政府および業界のパートナーが悪意あるサイバー活動に関する情報を受け取り、共有するための双方向情報共有プラットフォームです。
- ASD-ACSCはインフォスティーラーの活動を追跡しており、CTISプラットフォームを通じて、現在稼働中のコマンド&コントロールインフラに関する詳細情報を共有しています。
- パートナーに登録し、サイバー犯罪の脅威から組織や顧客データを守る。

侵害発生に備える

- インフォスティーラーによる侵害が発生した場合に備え、サイバーセキュリティインシデント対応計画を策定する。不審なファイルをダウンロードした疑いがある場合に、従業員が何をすべきか、誰に連絡すべきかを周知する。

ASD-ACSCの「エッセンシャルエイト」を導入する。

- 上記の対策に加え、ASD-ACSCは「エッセンシャルエイト」の残りの部分についても実施することを強く推奨しています。

リモートワークする従業員へのアドバイス

- 個人用デバイス上の情報を保護する
  - サイバー衛生（基本的なセキュリティ習慣）を身につけ、疑わしいリンクやポップアップをクリックしたり、未知または信頼できないソースからファイルやソフトウェアをダウンロードしたりしない。
  - 仕事用アカウントと個人用アカウントには異なるパスワードを設定する。可能な限り、個人アカウントにもMFAを設定する。
  - 雇用主から明確な許可がない限り、仕事用の認証情報を個人のパスワードマネージャーに保存しない。これには、ウェブブラウザのパスワードマネージャーも含まれる。**不安がある場合は、企業が管理するパスワードマネージャーの提供を雇用主に要請する。**
  - 共有または共用のワークステーションからは、仕事用アカウントにログインしない。
  - ウェブブラウザの自動入力機能に何が保存されているかを把握する。インフォスティーラーは、ブラウザが自動入力フォームに保存しているデータを標的にします。ウェブフォームに入力する際は、クレジットカード番号などの機密情報をブラウザの自動入力機能に保存するのではなく、手動で入力することを検討する。
  - インフォスティーラーによる情報窃取のリスクを低減するため、ブラウジングセッション終了後はすべてのオンラインサービスからログアウトし、ブラウザのクッキーを削除する。
  - 使用しているオペレーティングシステムに標準搭載されているウイルス対策機能を有効にする。サードパーティ製のウイルス対策ソフトを使用する場合は、信頼できるベンダーの製品であることを確認し、常に最新の状態に保つ。

サポート

インフォスティーラーによる侵害の影響を受けた、または対応支援を必要とするオーストラリアの組織は、ASD-ACSCに**1300 CYBER1（1300 292 371）**まで連絡するか、以下のウェブサイトから報告を提出してください：cyber.gov.au/report

ASD-ACSCは、たとえインシデントが制御下にあると考えられる場合でも、インフォスティーラーに関連する不審なネットワーク活動や「侵害の痕跡」について報告するよう、各組織に呼びかけています。ご提供いただいた情報は、サイバー脅威アクターの戦術・技術・手順に関する理解を深めるために活用され、同様の手口で標的となった他のオーストラリアの組織への注意喚起に役立てられます。

免責事項

このガイドブックの内容は一般的なものであり、特定の事情や緊急事態においては 法的な助言や依存すべき助言とみなされるべきものではありません。重要な事柄については、独立した専門家からご自身の状況に則した適切な助言を仰ぐべきです。

このガイドブックに含まれる情報に依存した結果として生じた損害、損失や費用に対して豪連邦政府はいかなる責任も負いません。

著作権

豪連邦政府紋章の使用について

豪連邦政府紋章の使用が許される条件については首相内閣省ホームページに掲載の「連邦政府の紋章に関する情報および指針」(pmc.gov.au)に詳述があります。

さらに詳細な情報について、またはサイバーセキュリティ事件の報告は以下の連絡先まで:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

この電話番号はオーストラリア国内でのみご利用いただけます。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre